United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

INTERNET ACCESS:

HOW TO DESIGN AND TEST AN INTERNET USE/MANAGEMENT POLICY

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Doris P. Montgomery
Major, U. S. Army

AY: 2000-2001

Mentor: _____
Approved: _____
Date: _____

Mentor: _____
Approved: _____

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
2002	N/A	-

Title and Subtitle How to Design and Test an Internet Use/Management Policy	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes
The original document contains color images.

Abstract
The Internet is filled with tremendous marketing potential and vulnerabilities, organizations should develop polices that offer both Internet Usage/Management policies that are consisted with their organization. A small sample from eight organizations will be surveyed using a prototype Internet policy model. The goal of this research is not to evaluate the organizations Internet policy but rather to demonstrate the prototype model in use. The scope of this study is limited, however it provides a model and a framework for evaluating organizational Internet management policies. However, additional work is required to provide statistics that can be used on a large scale to make definitive conclusions for any particular organization.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU

Number of Pages
46

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. agency use only *leave blank)* 2. report date 3. report type and dates covered

STUDENT RESEARCH PAPER

4. title and subtit

INTERNET ACCESS: HOW TO DESIGN AND TEST AN INTERNET USE/MANAGEMENT POLICY

5. funding numbers

N/A

6. author(s)

MAJOR DORIS p. MONTGOMERY
US ARMY

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC COMMAND AND STAFF COLLEGE
2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068

8. performing organization report number

NONE

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SAME AS #7. 10. sponsoring/monitoring agency report number:

NONE

11. SUPPLEMENTARY NOTES

NONE

12a. distribution/availability statemen

NO RESTRICTIONS

12b. distribution code

N/A abstract *(maximum 200 words)* **Today's challenge is for organizations to draft and adopt sensible e-mail policies that protect the organization against liability and at the same time encourage users to maximize benefits. A prototype model was developed to measure the effectiveness of the organization's Internet policy. This study provides a**

model and a framework for evaluating organizational Internet management policies. The purpose is to give the military an internet usage/management policy model that could be used to evaluate the effectiveness of any organization's policy. The scope of this research is limited to e-mail and internet use/management policy in an organization. Research indicates that e-mail and security are adjoining subjects when discussing internet access; therefore this project will include both e-mail and security as functions of internet access.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH)

INTERNET ACESS: DESIGN AND TEST INTERNET POLICY 15. NUMBER OF PAGES: ***43*** 16. PRICE CODE: N 17. SECURITY CLASSIFICATION OF REPORT

UNCLASSIFIED 18. security classification OF this page:

UNCLASSIFIED
19. security classification of abstract

UNCLASSIFIED 20. limitation of abstract

Date: _____

DISCLAMIER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY, REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

EXECUTIVE SUMMARY

Title: Internet Access: How to Design and Test an Internet Use/Management Policy.

Author: Doris P. Montgomery, MAJ, U.S. Army

Thesis: The Internet is filled with tremendous marketing potential and vulnerabilities, organizations should develop polices that offer both Internet Usage/Management policies that are consisted with their organization. A small sample from eight organizations will be surveyed using a prototype Internet policy model. The goal of this research is not to evaluate the organization's Internet policy but rather to demonstrate the prototype model in use. The scope of this study is limited, however it provides a model and a framework for evaluating organizational Internet management policies. However, additional work is required to provide statistics that can be used on a large scale to make definitive conclusions for any particular organization.

Background: Today's challenge is for organizations to draft and adopt sensible e-mail policies that protect the organization against liability and at the same time encourage users to maximize benefits.[1] A prototype model was developed to measure the effectiveness of the organization's Internet policy. This study provides a model and a framework for evaluating organizational Internet management policies.

Recommendation: An Internet policy can be very effective in the workplace. Organizations must implement a sound Internet usage/management policy that is consistent with their organizational structure. Organizations should also protect themselves from legal liabilities associated with inappropriate Internet use. However, most organizations trust their employee's common sense to do what is expected of them, meaning they trust them to stay away from inappropriate sites on the Internet. However, some organizations do allow employees to "surf" the Internet for personal reasons, either at lunch or after work. Most of the organizations I surveyed may need to improve their Internet usage policy. If an organization has a policy, then they should consider enforcing the policy or strengthening the policy. They can enforce the policy by communicating it to each employee by having them read and sign the policy agreement. Any organization using the Internet should develop a policy to manage its access by employees. This paper describes the areas that such an Internet management policy should contain. The paper then develops a model to evaluate the effectiveness of an organizations Internet management policies and demonstrates how to use the model with a small sample of organizations. Finally, additions to this research are described that would extend the model for wide-scale application.

---

[1] Software and Information Industry Association (SIIA), URL: < http://www.siia.net/glance/default.asp>, 10 October 2000.

TABLE OF CONTENTS

1 LIST OF ILLUSTRATIONS

Figures

Tables

2 DEFINITIONS AND ABBREVIATIONS

Table 1 Definitions and Abbreviations

IMO	Information Management Officer
IT	Information Technology
DISA	Defense Information Systems Agency
MCCSC	Marine Corps Command and Staff College
PERSCOM	Total Army Personnel Command
PERSINSD	Personnel Information Systems Directorate
TCP/IP	Transfer Control Protocol/Internet Protocol
DCSPER	Deputy Chief of Staff for Personnel
P & D	Pauline and Duke Inc.
USERID	user identity
LAN	Local Area Network
DISC4	Directorate of Information Systems for Command, Control, Communications
CGSC	Command and General Staff College
Surf the Internet	Traveling from one internet site to another.
Browser	A client program (software) that is used to look at various kinds of Internet resources.
E-mail	(Electronic mail) Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses (mailing list).
Internet (big I)	The vast collection of inter-connected networks that uses the TCP/IP protocols.
Internet (little i)	Anytime you connect 2 or more networks together, you have an internet.
Login or Logon	The account name used to gain access to a computer system (noun). The act of entering into a computer system (verb).

3 Introduction

We are living in what might be termed an "Information Age," an era characterized by the accelerating growth of collecting, processing and disseminating information. The Internet provides organizations with a global pipeline to move information at a high rate of speed with a significantly lower cost than previous communication means. With all those benefits, though, there are still some dangers and downsides. Here are a few of them: Time wasting and lost productivity, worry about the employees who are new to the web, and computer viruses. Network administrators live in fear of these dangers, because one nasty virus can disable an organization's entire network. Organizations must have an Internet Use Policy and some general guidelines.
Guidelines should include, but are not limited to the following:

1. Who can have Internet access?
2. When can they have access?
3. Why they have access?
4. How supervision will be handled?

An effective Internet Use Policy/Internet Management Policy should be specific. The policy should outline what sort of behavior is acceptable and what is not, along with what happens to employees who violate the policy. This paper will use Elron's Internet Manager Policy model and Ken Wasch's E-mail and Internet Policy as a baseline. The goal is to develop an Internet policy model and use it with a limited sample of organizations to test the model. The scope of this study is limited, however it provides a model and a framework for evaluating organizational Internet management policies. Elron Software Company enables organizations and service providers to maximize the use of the Internet with such software as their Internet Policy Manger (IPM). Internet Policy Management is a comprehensive set of solutions that allow organizations and service providers to maximize the productive use of the Internet and effectively manage associated risks. With worldwide headquarters in Burlington, Massachusetts, Elron Software has 120 employees and

is a private company.[2] Their product line provides:

1. Web access control
2. Electronic message content filtering
3. Virus protection
4. Network security

Internet Manager's products enable organizations to develop, implement and manage Internet Usage Policies (IUPs) based on the unique needs of their organization. By managing Internet access, reducing recreational "surfing," and blocking "spam," viruses and other inappropriate electronic communications, the products help to:

1. Boost productivity
2. Protect confidential information
3. Reduce network congestion
4. Limit legal liability[3]

Ken Wasch is the President of Software and Information Industry Association (SIIA), headquartered in Washington, DC. SIIA has brought together companies of the software and information industry, expanding market opportunities and forged the way toward a stronger industry. SIIA works towards building the digital economy. SIIA is a trade association with a global reach that provides an integrative voice for all businesses that provide software and information to the digital economy. SIIA provides a neutral business forum for members to understand business models, technological advancements, industry trends and "best practices."[4] Mr. Wasch developed an E-mail and Internet Policy for his company, based on this policy model. According to Mr. Wasch, an organization Internet/e-mail policy can cover a range of communication media: internal and external e-mail, Internet use, computers, voice mail, faxes, paper-based documents and files, and any other communication media. In general, however, all policies should emphasize the business purpose of these media, notify employees about privacy,

---

[2] Elron Internet Manager, URL: <http://www.elronsoftware.com/productfamily/overview.shtml>, accessed 25 September 2000.
[3] Elron Internet Manager, URL: <http://www.elronsoftware.com/productfamily/overview.shtml>, accessed 25 September 2000.
[4] Software and Information Industry Association (SIIA), URL: < http://www.siia.net/glance/default.asp>, 10

identify appropriate and prohibited uses, and address system security issues. What to Include in Your Policy? Use the checklist below to identify topics to cover in your policy.[5]

Step 1: Permission to monitor

Step 2: What to permit, what to prohibit

Step 3: Alert employees

Although many organizations have given their employees Internet access, not all have considered the impact access can have on corporate liability, reputation, and employee productivity. Today's challenge is for organizations to draft and adopt sensible e-mail policies that protect the organization against liability and at the same time encourage users to maximize benefits.[6]

October 2000.

[5] Software and Information Industry Association (SIIA), URL: < http://www.siia.net/glance/default.asp>, 10 October 2000.

[6] Software and Information Industry Association (SIIA), URL: < http://www.siia.net/glance/default.asp>, 10 October 2000.

4 SITUATION ANALYSIS

4.1.1 Background

In today's information intensive world, organizations must use the Internet to conduct business in order to remain competitive. The Internet is a network of networks, which has established methods of communication. The Internet is the world's largest collection of networks and reaches universities, government labs, commercial enterprises, and military installations in many countries.[7] The Internet provides an electronic medium that is becoming increasingly essential for organizations to conduct business. Without access to the Internet, the Army and many other organizations could easily lose a strategic advantage in their core business area. The Internet provides organizations with a global pipeline to move information at a high rate of speed with a significantly lower cost than previous communication means. Organizations are constantly upgrading their information architectures to maximize their benefit from the Internet. Organizations are also encouraging their personnel to use the Internet to gain a business advantage.

Electronic mail (email) instantly connects employees across the country, or around the world, enhancing communication and collaboration. "Surfing" the Internet can also bring huge amounts of data and information directly to a person's desktop. This can facilitate problem solving and the creation of new ideas in support of the organization. In general, they are providing employees and soldiers with the tools and the freedom to become more technologically proficient. However, as more and more organizations merge onto the information superhighway and upgrade their equipment, they find themselves faced with new problems. The Internet, while providing a powerful medium for business, can also provide serious vulnerabilities. Like the Army, most organizations are quickly realizing that encouraging employees to use e-mail and to "surf" the Internet requires constraints to ensure these tools are not abused. Many organizations are finding that new management policies are needed to control access to the Internet and to ensure that it is used to

[7] Howard, John D. (1997). *An Analysis Of Security Incidents On The Internet* 1989 - 1995. Ph.D. diss., Carnegie Mellon University.

enhance corporate productivity.

4.1.2 Policy

The management problem associated with Internet access is a policy issue. Most organizations after making the move to a high technology environment are just beginning to realize the magnitude of their problem. Policies to govern use of the Internet are usually included in existing communications policy for the organization. These policies, however, are generally not sufficient to manage such an innovative technology as the Internet. The biggest problem is determining the right amount of control without inhibiting individuals from becoming more familiar and proficient with the Internet. Most organizations are taking steps to improve their information technology infrastructure and encourage employees to become more familiar with the system. This proactive approach is imperative in today's business society where electronic mediums are becoming the standard way of business. However, organizations must also provide policy to govern the use of these tools to prevent corporate embarrassment or compromises to critical business information.

4.1.3 Security

When an organization writes policy, security should be a primary consideration. Security of the organization's information system can easily be compromised by a user's ability to access websites and download potentially destructive viruses. Additionally, security must account for unauthorized users trying to enter the system. These security risks can be managed using software and hardware tools, but effective corporate policies are also essential to ensure the success of these tools.

4.1.4 Premise

Most organizations have policies that govern Internet use, however, these policies are often included as part of their communications guidelines. These policies are dramatically outdated by new information technology capabilities and will no longer support many organization's management

objectives. Each of the eight organizations reviewed in this paper has a communications policy. However, these policies need to be more Internet specific. If an organization such as the Army's personnel management agency constructs a new communications policy using documented and proven Internet guidelines and enforces the policy, then the organization will be able to manage Internet access to support corporate objectives.

4.1.5 Scope

The purpose is to give the military an Internet usage/management policy model that could be used to evaluate the effectiveness of any organization's policy. The scope of this research is limited to e-mail and Internet Use/Management policy in an organization. Research indicates that e-mail and security are adjoining subjects when discussing Internet access; therefore this project will include both e-mail and security as functions of Internet access.[8] Because of the nature and sensitivity of its business, I will focus particularly on the U.S. Total Army Personnel Command (PERSCOM) throughout this project. PERSCOM's mission is to manage the Army's Personnel Management system, to include assignment and career management of officers, noncommissioned officers, and enlisted soldiers worldwide, to meet Army requirements. The project will use the Internet Use/Management Policy model as a template to evaluate the Internet policies of PERSCOM and seven other the sampled organizations. Using this evaluation, it will provide an analysis regarding proper Internet Use/Management in any organization.

4.1.6 The U.S. Total Army Personnel Command (PERSCOM) and the Internet

PERSCOM is the U. S. Army agency responsible for personnel management. PERSCOM uses the Internet for conducting a wide range of business processes including e-mail, website usage, and transmission of data to other U. S. Army agencies around the world. The Internet provides an extremely efficient medium for PERSCOM to send and receive information concerning the

[8] Wasch, Ken, 1997, E-mail and Internet Policy, Association *Management,* 1 May 1997, URL:

management, movement, and status of soldiers worldwide. While the Internet provides an efficient medium for conducting business, it also provides some management challenges. The majority of these challenges are covered by PERSCOM policy. However, by developing an Internet specific policy, PERSCOM can better manage its information technology assets.

4.1.7 Organization

PERSCOM consists of four directorates and each of these directorates has its own information network. The Personnel Information Systems Directorate (PERSINSD) is one of PERSCOM's four directorates. This directorate manages telecommunications for all four of the directorates. Each directorate has an Information Management Officer (IMO) who manages the directorate's information system. PERSINSD is responsible for ensuring the entire organization and the individual directorates have the telecommunications required to conduct operations. The requirements include network management, website management, e-mail and Internet browsing capabilities. In addition to providing these services, PERSINSD, has the responsibility for drafting and managing the policy that governs these services. PERSCOM has approximately 3400 workstations, most of which have Internet connectivity. Users access the Internet for many purposes. The largest use is e-mail, however, users can browse the Internet virtually unrestricted using browser software installed on their desktop computers. Controlling this unrestricted access provides a huge management challenge for PERSINSD. The solution is to create a realistic policy that defines reasonable, enforceable rules for email and Internet browsing.

4.1.8 Work Plan

To obtain information on this subject, I conducted secondary research on numerous sources. These sources included personal interviews with subject matter experts, numerous trips to libraries as well as use of the Internet. This process took about six weeks and provided the

---

<http://www.asaenet.org/newsletters/display/0,1901,249,00.html>, 15 October 2000

information required to construct an Internet policy model. After construction of the model, I began collecting primary research in order to provide an analysis of the eight organizations chosen for the project. I constructed a survey using policy guidelines and then e-mailed the survey to the eight organizations. It took about four weeks to collect and analyze the data. After completion of the analysis, I summarized the results and provided the conclusions and recommendations.

5 Secondary Research and Model

As the Internet continues to grow and more organizations merge onto the information superhighway, organizations will need to develop Internet policies to better use these information tools. Although many organizations have given their employees Internet access, not all have considered the impact Internet access can have on corporate liability, reputation, and employee productivity. Today's challenge for organizations is to draft and adopt sensible Internet policies that protect the organization against liability while at the same time encouraging users to maximize benefits.[9] Most Internet policies have common themes including the use of e-mail, Internet browser, and security. It is common to find all of these subjects in an umbrella type policy, which reflects the organization's philosophies as well as limitations on use of the Internet. To develop a good Internet policy, an organization must first develop a guideline defining how they want to proceed with their policy development. Individuals, not just IMOs, who manage, implement, control and use the systems, should work as a team to develop this policy. Once the guidelines are defined, and the policy approved the organization must enforce the policy.

The Internet Management Policy model (See Figure 1) will be used as a template for evaluating the Internet policies of sampled organizations. Representatives from each organization will be questioned to determine the extent that Internet access is managed within the organization. The result of these surveys will be tabulated to provide insight into Internet management concerns for any organization.

[9] Wasch, Ken, 1997, *E-mail and Internet Policy*, Association Management, 1 May 1997, URL: <http://www.asaenet.org/newsletters/display/0,1901,249,00.html>, 15 October 2000

5.1 BASELINE FOR AN INTERNET POLICY

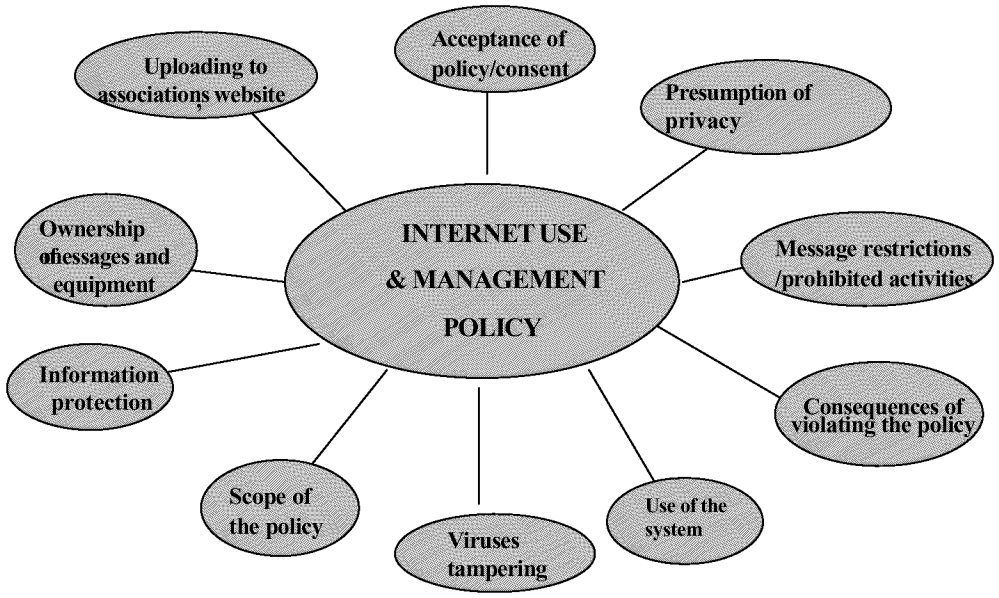

Figure 1 Baseline for an Internet Policy[10]

5.1.1 Scope of the policy

The scope should provide the specifics of what is covered in the policy. The purpose of the policy is to implement guidelines for the use of computer network resources, including Local Area Networks (LAN), the Internet, and e-mail by the employees of an organization. The policy should set forth Internet usage restrictions that are necessary to reduce potential liability, risk of inappropriate use, and possible adverse perceptions by the general public.

[10] Wasch, Ken 1997, *E-mail and Internet Policy*, Association Management, 1 May 1997, URL: <http://www.asaenet.org/newsletters/display/0,1901,249,00.html>, 15 October 2000

Internet and e-mail policies generally have three broad areas:

1. Privacy rights of the employee
2. Liability of the employer for employee Internet use
3. Protection of the employer's confidential information.[11]

5.1.2 Use of the system

This defines the organization's business objectives in using the Internet. The purpose of providing hardware and software to employees is to increase their productivity and enhance their knowledge. Some reasonable personal use should be allowed, but the key word is reasonable. Employees should understand that the organization has the right to determine what constitutes this reasonable amount of use. Personal use that includes excessive Internet browsing during work hours, football pools, jokes, pornography, purchasing stocks, political causes or creation of chain letters is generally considered unreasonable personal use.

5.1.3 Acceptance of policy/consent

Acceptance of the policy and consent to the terms is an important piece in the policy process. It is essential that employees and soldiers are aware of the policy, understand the policy, and that they agree to the terms of the policy. If they do not agree to the terms, they need to understand that constitutes grounds for termination of their workstation service as well as their employment. Acceptance of the organization's Internet policy should be part of every newcomer's inprocessing (An example of an Internet usage agreement is below). This agreement provides an additional reminder of the organization's policy. As an extra measure of protection, most experts recommend that Internet use policies include a statement signed by the employee that makes it clear that the employee has read and understood the Internet policy.

---

[11] Wasch, Ken, 1997, *E-mail and Internet Policy*, Association Management, 1 May 1997, URL: <http://www.asaenet.org/newsletters/display/0,1901,249,00.html>, 15 October 2000

Internet Usage Agreement

On _____ (date), I _____ (print name) received a copy of the Internet Usage Policy. I have read and fully understand the terms of this policy and agree to abide by them. I realize that the xxxx may incorporate monitoring software and may record, the Internet address of any site I visit for management's use. I understand that failure to adhere to this policy may result in discipline, up to and including termination. I have read, understand and agree to comply with the Xxxx's Internet usage policy:

(Signature)_____(date) _____

A copy of this statement will be filed with your personnel records.

Additionally, organizations can use software management tools that provide a "pop-up" message during login procedures.

5.1.4 Presumption of privacy

The organization's policy should be very clear in this subject: employees should have no presumption of privacy. Employees need to understand that the organization can monitor the use of corporate information technology infrastructure, e-mail and Internet connections any time. Violation of the organization policy regarding Internet use may result in disciplinary action up to and including dismissal.

5.1.5 Consequences of violating the policy

This defines what will happen if the employee violates the policy. Employees need to understand the impact of their actions if they violate Internet policy. Violation of policy may result in disciplinary actions, depending on the severity or frequency of the violations. Disciplinary actions could include:

1. Counseling statements for policy violations.

2. A suspension/termination of Internet or e-mail privileges.
3. Termination of employment.
4. Access may be restricted

5.1.6 Ownership of messages and equipment

This falls into the realm of corporate data and ownership. In this case, the organization's policy needs to be clear in stating that the workstation, software, and all related hardware items are corporate assets. Additionally, all messages or information created at the workstation belong to the employer and are subject to monitoring. By making this clear in the policy, the organization shields itself against possible violation of privacy issues and charges.

5.1.7 Message restrictions/Prohibited activities

This defines subject matter that is not allowed during e-mail sessions or while Internet browsing. Personnel must understand the implications of messages that might be defamatory, offensive, harassing or disruptive. Messages containing such content could create employee or organization liability. Employees must also understand the detrimental results of downloading prohibited material through an Internet browser. While pornography is probably the most common prohibited material, other materials such as copyrighted information, trade secrets, or confidential material can also bring actions against the employee or the organization. The policy should be very specific about what materials are prohibited.

5.1.8 Information protection

This defines information that is sensitive to the organization and provides guidelines on handling this information when accessing the Internet. Each person needs to understand the value of such information and the advantage it may provide to others outside the organization. Employees may not realize how easy it is to intercept information on the Internet. This is an education process

and policies that explain and define this subject are essential to the organization. This includes protection from viruses as well as security of organizational information. Employees should keep personal passwords confidential and change passwords on a regular basis as instructed by the organization IMO. Failure to adhere to this policy jeopardizes network security. The organization reserves the right to review employee Internet, LAN, on-line services and e-mail use to determine whether the system's use is appropriate and conforms to the organization's policy. If an employee is found to be not conforming to any section of this policy, the management has the choice to remove the employee's access to the computer network resources or to proceed with other disciplinary actions.

5.1.9 Viruses/tampering

This is closely related with downloading of prohibited material. Most viruses penetrate networks through Internet access. This is an education process and employees need to learn the impact of viruses and the office to contact in the event of a virus infection on their workstation. A virus is prominent and care must be taken not to contaminate any computers in the organization. A virus checker should be running on computers that are connected to the Internet, to check downloaded files, e-mail, and attachments. Employees are responsible for virus checking of downloaded files.

5.1.10 Uploading to the organization's web site

The organization must have procedures for updating the organization's website. A good way to keep a web site functional is to have all material channeled through a central person or section for content screening and technical update. This prevents unauthorized materials from being exposed to other Internet browsers and possibly causing embarrassment or liability to the organization.

6 PRIMARY RESEARCH

6.1 Survey of Internet Policy

The intent of my research is not to evaluate the organization's Internet policy to see who has a good policy. The intent of this research is not to evaluate the organization's Internet policy but rather to demonstrate the prototype model in use. The scope of this study is limited, however it provides a model and a framework for evaluating organizational Internet management policies. However, additional work is required to provide statistics that can be used on a large scale to make definitive conclusions for any particular organization. This research will develop a prototype model and demonstrate its use to determine if the sampled organizations have an Internet policy and if their employees are aware of the policy. This paper will use Elron's Internet Manager Policy (IMP) model and Ken Wasch's E-mail and Internet Policy as a baseline. Elron Software has had great success with over 3,500 organizations, using a model similar to Ken Wasch's Internet policy model. They provide solutions for website access control, electronic messaging, content filtering, virus protection and network security.[12] I created a survey of questions using the Internet Management Policy model as a baseline. I used e-mail to conduct the surveys with great success. Seven organizations were surveyed, as well as users in PERSCOM. The target organizations consisted of government as well as civilian organizations. The intent is to demonstrate the use of the Internet policy model, by conducting a limited survey of the sampled organizations. Copies of the organization's policy were obtained, which provided additional support for the comparison.

The purpose of the model is to explain, in a practical way, an Internet Management Policy that is effective and can be used by government agencies and civilian organizations. The results of the survey are compiled in ten tables (See Tables 2-11). PERSCOM was discussed earlier; a brief description of the seven other surveyed agencies is listed below.

[12] Elron Software, Internet Manager, Burlington, Massachusetts, URL: <http://www.elronsoftware.com>, accessed 5 November 2000

a. The Defense Information Systems Agency (DISA), headquartered in Arlington, Virginia is a large and complex defense communications organization. DISA's networks support 7000 plus user circuits at 325 locations.[13]

b. U.S. Army Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4), headquartered in the Pentagon has worldwide responsibilities for Department of the Army requirements. They have a large number of communications requirements that require use of the Internet including e-mail. They use both, secret and unclassified local area networks (LAN) in their local headquarters. The local unclassified LAN has access to the Internet.[14]

c. U.S. Army Office of the Deputy Chief of Staff for Personnel (ODCSPER), headquartered in the Pentagon. Develops integrated human resources strategies and make decisions about the Army's personnel structure, acquisition, distribution, development, deployment, sustainment, compensation, and transition, enabling the Army to prepare for and conduct military operations today and simultaneously regenerate itself for tomorrow.[15]

d. U.S. Army Command and General Staff College (CGSC), located at Fort Leavenworth, Kansas is the recognized keystone of the Army's school system. Internal to CGSC is the Directorate of Technology (DOT) that is responsible for managing the planning, development, coordination, implementation and security of CGSC automated information systems. DOT is also responsible for training students in the use of GCSC automated information systems. DOT has in excess of 1300 Desktop workstations, and 250 laptop computers that are connected via an internal network. This network has access to the Internet via multiple modem connections.[16]

e. Marine Corps University Command and Staff College (MCUCSC), headquartered in Quantico, Va. The Marine Corps University develops the professional competence of its Marine, other service, international, and civilian students who attend its eight component schools. As the Marine Corps proponent of professional military education, the University focuses on the leadership, warfighting, and staff development skills of the nation's military forces through resident and distance learning programs. Graduates of its colleges and schools are prepared to perform with increased effectiveness in service, joint and multinational environments at the tactical, operational, and strategic levels of war, as well as in crises ranging from humanitarian assistance to combat. MCUCSC is staffed with an Information Systems Management Officer and a host of information system coordinators, visual information specialist and computer support.[17]

f. Pauline & Duke, Incorporated (P&D, Inc.), headquartered in Honolulu, Hawaii. P&D, Inc. is a

---

[13]Defense Information Systems Agency, URL: < www.disa.mil/handbook/references.html>, accessed 27 December 2000.

[14]Office of the Director of Information Systems for Command, Control, Communications (DISC4), URL: <http://www.army.mil/disc4/index.html, > 15 December 00.

[15]Office of the Deputy Chief of Staff for Personnel (DCSPER), Pentagon, URL: <http://www.odcsper.army.mil>, accessed 5 December 00.

[16]Farnell, Angie, MAJ, U.S. Army Command and General Staff College, Student, Leavenworth, Ks, interview with author, Oct 5, 2000

[17] Marine Corps University Command and Staff College, Quantico, Va., URL: <http://www.mcu.usmc.mil/csc/default.htm>, accessed 22 November 2000.

national marketer, researcher and processor of information both on and off-line. Pauline & Duke are destined to be one of the largest providers of needed information. Through its portfolio of services, Pauline & Duke provides unprocessed researched for Attorneys and Paralegal, Investigators, Screening & Search Firms, Credit & Collection Professionals, Process Servers, and Information Brokers. The Company also provides information to businesses in other industries, which gives them the edge to grow. The company's source structure is the key to servicing the industries demand for information. Pauline & Duke sources more than ten (10) different providers and over six hundred databases with more than one hundred fifty million files on record. Pauline & Duke are among the most sophisticated and technologically advanced information providers in the state of Hawaii.[18]

g. Pillsbury Company, headquartered in Minneapolis, Minnesota, specializes in consumer foods and baking products. The company uses local area networks at each of satellite locations worldwide. A central IT network system located at the company headquarters manages these Intranets.[19]

[18] Pauline & Duke, <www.http: //64.176.205.126/PR1223/default.htm>, accessed 22 November 2000.
[19] Pillsbury Company, headquartered in Minneapolis, Minnesota, < http://www.pillsbury.com>, accessed 20 November 2000.

7 Analysis

7.1 Qualitative Analysis

As part of this project, I conducted a qualitative and quantitative analysis of eight organizations using Internet Use/Management Policy model. The qualitative analysis is derived from a descriptive survey sent to each of the seven organizations as well as to three users in PERSCOM (See Appendixes 1-13). The results of this survey are compiled in a matrix. The rules for the survey are Y (yes), covered in the policy, N (no), not covered in the policy, and U (undetermined) the individual was unsure of whether the organization's policy covered the subject. Additionally, I was able to obtain policies from six of the eight organizations. Information derived from the policies combined with the surveys was used for a comprehensive analysis of those organizations (See Tables 2-11). The results from the quantitative analysis can be found in tables 11 and 12.

Table 2 MATRIX SHOWING RESULTS OF COMPARISON BETWEEN IINTERNET USE POLICIES VERSUS CURRENT ORGANIZATION POLICIES REGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
PERSCOM	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
DISA	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
DISC4	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
CGSC	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
DCSPER	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
MCUCSC	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
P&D	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
PILLSBURY	U	N	N	N	Y	Y	Y	Y	Y	N

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.2 PERSCOM versus Internet Use/Management Policy Models

The results of the PERSCOM analysis were obtained through use of the organization's policy as well as through the use of three user surveys. These surveys combined with the organization's policy provided additional information for comparison (See Table 3).

PERSCOM has two Internet policy documents that govern their Internet and e-mail use. These are comprehensive polices that cover the use of all communication mediums. However, when compared to the Internet Use/Management Policy model, they have some shortfalls such as ownership of data and upload to the website. These subjects are not covered in either policy and PERSCOM needs to provide clarification and guidelines on these subjects.

PERSCOM used a process of organizing a chain-teaching program for IMOs and supervisors who in turn, train users on issues related to the use of the Internet. This is an excellent approach, which will ensure employees are aware of the rules regarding use.

Table 3 MATRIX SHOWING RESULTS OF PERSCOM POLICY SURVEY REGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
PERSCOM POL	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
USER 1	Y	Y	Y	N	Y	N	Y	N	Y	N
USER 2	Y	Y	Y	Y	Y	N	Y	Y	Y	N
USER 3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.3 DISA versus Internet Management Policy Model

The combination of the organization's policy with a user survey provided the information for the DISA comparison (See Table 4). The user has a background in computer science. The results of this survey reflect her background because DISA's policy is extremely generic. However, DISA

is generally staffed with computer literate personnel, therefore, some inherent knowledge regarding Internet use is infused in the organization.

DISA was strong across the spectrum of the Internet policy model. The only area where DISA did not receive a yes was in ownership of data. DISA is a worldwide organization with many users. Information that travels over DISA's systems and networks may come from any of the DoD agencies, therefore, DISA cannot necessarily lay claim to all information on their network. Neither their policy nor the survey showed clear guidance on this subject. In all other areas, DISA's policy or their employee's inherent knowledge of networks and information technology systems, resulted in clear understanding of the other rules of the Internet Policy model.

Table 4 MATRIX SHOWING RESULTS OF DISA POLICY SURVEY REGARDING INTENET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
DISA	Y	Y	N	Y	N	N	Y	Y	Y	Y
USER #1	U	Y	Y	Y	Y	N	Y	Y	Y	Y

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.4 ODISC4 versus Internet Management Policy Model

The combination of the organization's policy and user surveys provided the information for ODISC4's survey (See Table 5). ODISC4 has a communication policy that encompasses Internet and e-mail use, however, the policy is not detailed enough to protect the agency in its classified mission. This organization is a prime example of an organization with a lot to lose if policy regarding use of the Internet is not enforced. However, due to the technical background of the majority of

employees, the organization benefits from their inherent knowledge. The specific area where the organization needs improvement is uploading to the website. This area could create a substantial security risk to the organization and should probably be reviewed.

Table 5 MATRIX SHOWING RESULTS OF ODISC4 POLICY SURVEY REGARDING INTERNET USERS

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
ODISC4 POLICY	Y	Y	Y	Y	Y	N	Y	Y	Y	N
USER#1	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
USER#2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USER#3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.5 ODCSPER versus Internet Management Policy Model

The results of ODCSPER's survey were developed using one survey (See Table 6). However, due to the mission of ODCSPER, I believe Internet policy is a critical part of their security program; therefore, the employees should have a good knowledge of the organization's policy. On the other hand, due to the size and nature of this organization, the survey probably did not attained perfection in determining the organization's effectiveness in controlling Internet use. Nevertheless, I am using this information to measure ODCSPER and its Internet policy with those limitations in mind.

Table 6 MATRIX SHOWING RESULTS OF ODCSPER POLICY SURVEY REGARDING INTENET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
ODCSPER	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
USER #1	U	Y	Y	N	Y	N	Y	Y	Y	N

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.6 U.S. Army CGSC versus Internet Management Policy Model

The results of the CGSC survey were derived solely from policy and a user survey and an interview with the surveyed individual (See Table 7). Subject material at CGSC is comparable to university advanced degree programs; therefore, a huge focus for CGSC is making students more technically competent. This benefits the information technology managers at CGSC because students begin to realize the importance of the Internet as a tool as well as the consequences of its misuse. The CGSC has a website and requires students to access this site to download class assignments and information. Additionally, CGSC provides each student with an e-mail account, which is CGSC's primary means of information distribution. Clearly, CGSC needs an extensive, well-publicized policy to maintain control of their transient population of users. The surveyed student's input, demonstrates that CGSC has a policy in place and that students are familiar with the policy. When compared to the Internet Use/Management Policy model, they have many strong areas. Those areas include use of the system, acceptance of the policy, presumption of privacy, consequences of violation, message restriction and prohibited activities and information protection. The CGSC policy also has some weak areas that include scope of policy and upload to website.

Surprisingly, CGSC did well in acceptance of policy, indicating that students know and understand the policy. This is a credit to the CGSC technical staff and is somewhat unexpected given such a transient user base.

Table 7 MATRIX SHOWING RESULTS OF USACGSC POLICY SURVEYREGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
CGSC POLICY	U	Y	Y	Y	Y	N	Y	Y	Y	N
USER	U	Y	Y	Y	Y	Y	Y	Y	Y	N

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.7 MCUCSC versus Internet Management Policy Model

The results of the MCUCSC survey were developed using two surveys (See Table 8). Both individuals possess some knowledge of the Internet and computer technology. However, due to the MCUCSC's mission, I believe computer policy is a critical part of their security program; therefore, the students probably have a good knowledge of the organization's policy. On the other hand, due to the size and nature of this organization, the survey is probably not attained perfection in determining the organization's effectiveness in controlling Internet use. Nevertheless, I am using this information to measure the MCUCSC and it's Internet policy with those limitations in mind.

The MCUCSC received a no in one area: upload to the website. Upload to website is a deficiency that is not too serious and can be corrected by establishing guidelines on how to provide information for uploading to the website. After guidelines are established, e-mail can be sent to all students advertising the procedures.

Table 8 MATRIX SHOWING RESULTS OF MCUCSC POLICY SURVEY REGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
MCUCSC POL	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USER#1	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
USER#2	U	Y	Y	Y	Y	Y	Y	Y	Y	N

Legend
Y-covered in policy
N-not covered in policy
U-undetermined by user

7.8 Pauline and Duke, Inc. versus Internet Management Policy Model

Only one employee was surveyed for P&D, Inc (See Table 9). P & D Inc. is a national marketer, researcher and processor of information both on and off-line. P & D Inc. sources more than ten (10) different providers over six hundred databases with more than one hundred fifty million files on record. This is a prime example of an organization with a lot to lose if its corporate information is not protected. I believe the inherent knowledge of their employees contributes to ensuring policy is managed. This is a benefit for companies such as P&D, Inc.

The only area where P&D, Inc. did not receive a yes was acceptance of policy. This deficiency can easily be corrected. The organization must have employees sign a policy waiver and use software with a message indicator capability reminder.

Table 9 MATRIX SHOWING RESULTS OF PAULINE & DUKE, INC. POLICY SURVEY REGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
P&D, Inc. Policy	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
USER	Y	Y	N	Y	Y	Y	Y	Y	Y	Y

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.9 Pillsbury Company versus Internet Management Policy Model

The results of the Pillsbury survey come from one survey (See Table 10). I was not able to survey or interview an Internet technology professional from Pillsbury however, the individual who completed the survey is a customer service supervisor with a computer background.

Pillsbury did not do as well as other organizations in the study. They received no's in the areas of acceptance of policy, presumption of privacy, and uploading to the website. As mentioned in a previous organization's analysis, acceptance of policy and uploading to website are not critical deficiencies, however, presumption of privacy could be a particularly dangerous deficiency. Employees need to understand their computers can be monitored at any time with or without their expressed permission. Because Pillsbury is a purely commercial organization, this has the potential for serious damage should an employee initiate a privacy lawsuit against the company in relation to monitoring. The areas of consequences of violating policy, ownership of data, message restriction/prohibited activities, virus tampering and information protection are important areas for the company to do well. These are areas that could protect the company from providing critical information to competitors and thus reducing their strategic advantage. Additionally, Pillsbury

provided me with an information paper about recent employee termination over excessive or improper use of the Internet. Maybe the Internet policy model can assist Pillsbury in getting the word out to employees reference the consequences of violating the policy.

Table 10 MATRIX SHOWING RESULTS OF PILLSBURY POLICY SURVEY REGARDING INTERNET USE

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website
PILLSBURY	U	Y	N	Y	N	N	Y	Y	Y	Y
USER	U	Y	N	Y	Y	N	Y	Y	Y	N

Legend
Y - covered in policy
N - not covered in policy
U - undetermined by user

7.10 Quantitative analysis

The quantitative analysis for this project is derived from the results of the descriptive survey and policies obtained from the organizations. To obtain a quantitative result, I assigned weights to each of the policy model criteria according to my analysis of research throughout this project. I assigned a weight of 1 for a yes answer and a weight of 0 for a no or undetermined answer. I then multiplied the weights of the criteria and the weights of the answers. The sum of the products provides a total for the organization with higher values being better (See Table 11 and Figure 2). The following weights were assigned based on my review of relevant literature and my subjective judgment:

1. Scope of the policy - 1.5
2. Use of the system - 4
3. Acceptance of the policy - 3.5
4. Presumption of privacy - 3

5. Message restriction and prohibited activities - 4
6. Consequences of Violating policy - 5
7. Ownership of data - 2.5
8. Viruses and tampering - 2
9. Information protection - 3
10. Upload to Website - 1

Weights assigned to the answers of the survey:

1. Yes - 1
2. No - 0
3. Undetermined - 0

Table 11 MATRIX SHOWING RESULTS OF QUANTITATIVE ANALYSIS WITH WEIGHTS ASSIGNED TO CRITERIA

	Scope of Policy	Use of System	Accept Policy	Presump of Privacy	Conseq of Violating Policy	Ownership of Data	Message Restrict Prohibited Activ	Viruses Tamper	Info Protect	Upload to Website	TOTAL SCORE
Weight	***1.5***	***4***	***3.5***	***3***	***5***	***2.5***	***4***	***2***	***3***	**1**	
PERSCOM	Y(1.5)	Y(4)	Y(3.5)	Y(3)	Y(5)	N(0)	N(0)	Y(2)	Y(3)	N(0)	22
DISA	Y(1.5)	Y(4)	Y(3.5)	Y(3)	Y(5)	N(0)	Y(4)	Y(2)	Y(3)	Y(1)	27
DISC4	Y(1.5)	Y(4)	Y(3.5)	Y(3)	Y(5)	Y(2.5)	Y(4)	Y(2)	Y(3)	N(0)	28.5
DCSPER	Y(1.5)	Y(4)	Y(3.5)	N(0)	Y(5)	N(0)	Y(4)	Y(2)	Y(3)	N(1)	23
CGSC	Y(1.5)	Y(4)	Y(3.5)	Y(3)	Y(5)	Y(2.5)	Y(4)	Y(2)	Y(3)	N(0)	28.5
MCUCSC	Y(1.5)	Y(4)	Y(3.5)	Y(3)	Y(5)	Y(2.5)	Y(4)	Y(2)	Y(3)	N(0)	28.5
P & D, INC.	Y(1.5)	Y(4)	N(0)	Y(3)	Y(5)	Y(2.5)	Y(4)	Y(2)	Y(3)	Y(1)	26
PILLSBURY	U(0)	N(0)	N(0)	N(0)	Y(5)	Y(2.5)	Y(4)	Y(2)	Y(3)	N(0)	16.5

Legend	
Y - covered in policy	Y = 1
N - not covered in policy	N =0
U - undetermined by user	U = 0

Weight based on importance to Policy

5.0 high 1.0 low

BLUE - HIGH

RED - LOW

MEAN - 25

7.10.1 Sample Statistics

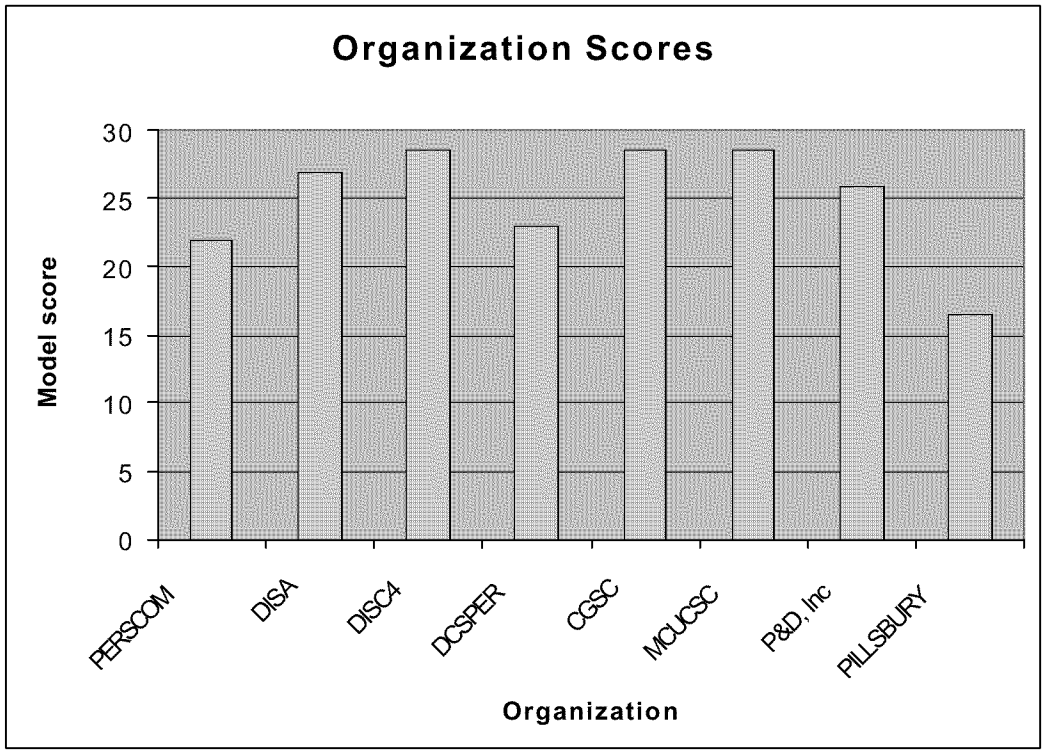

Figure 2 Organization Internet Management Policy Management Scores

Most of the organizations scored above 25.0 and several organizations scored close to the maximum value of 29.5 (See Figure 2). The Pillsbury Company is essentially an outliner in this sample with the only excessively low score relative to the other organizations. Consequently the data in this small sample are skewed and do not closely fit a normal distribution. Regardless, I will assume that the sample is taken from a population of organizations whose scores on the Internet management policy survey would be normally distributed.

The limited scope of this study provides a model and a framework for evaluating organizational Internet management policies but additional work is required to provide statistics that can be used on a large scale to make definitive conclusions for any particular organization. Table 11 illustrates the results of this survey.

The summary statistics for this project are listed in Table 12. Notice the confidence interval

listed in the last row of the table. This interval represents the range within which we can be 95% confident that the true value of the population mean lies. However, in this case the width of the confidence interval is very large, relative to both the range of possible values, and to the scores of the sampled organizations. This significantly limits the strength of the conclusions that the organizations can make based on their score. However, by sampling a larger number of organizations from the population (of all organizations) a confidence interval of any desired width and percentage can be generated.

Table 12 Sample Statistics

Mean	25.00
Median	26.50
Mode	28.50
Maximum	28.50
Minimum	16.50
Variance	18.14
Standard Deviation	4.23
95% Confidence Interval for the population mean	21.46/28.54/CI 7.09

The 95% confidence interval for the population mean shows the upper and lower values within which we are 95% confident that the true value of the population mean lies. In this case, I assume that the population variance is unknown, therefore, the formula for finding these values is $\overline{X} \pm t_{1-\alpha/2;n-1} \frac{S}{\sqrt{n}}$.[20] Substituting the values of the appropriate sample statistics yields $25 \pm 2.365 \frac{4.23}{\sqrt{8}} = (21.46, 28.54)$. Since the size of the sample in this study is fairly small, the 95% confidence interval is very large. The implications of this will be discussed further in the conclusion section. Returning to the scores for each organization on the Internet management policy survey, we

[20] R. Lyman Ott and Mendenhall, William, *Understanding Statistics*, Duxbury Press, c1994, 6th ed., 235

see that all organizations except one, achieved a score that falls within this 95% confidence interval. Overlooking for now the size of the confidence interval, we can conclude that all but this one organization achieved scores on the survey that could be considered average. However this is an extremely wide confidence interval, as acknowledged earlier, and the Pillsbury personnel surveyed scored over two standard deviations below the sample mean, which could clearly be a cause for concern.

Given the limited scope and time constraints for completing this study, a small sample size from the population of all organizations was used. By having a larger number of different organizations complete the survey we could achieve a confidence interval for the true value of the population mean with any degree of confidence, and any interval width. An organization using the model to assess their Internet management policies can make stronger conclusions if the confidence interval is narrower. For example a sample size of 278 would be required to obtain a 95% confidence interval that is less than one unit wide. Again, assuming that the population variance is unknown, the formula for the confidence interval width is $\left(\frac{2S}{\sqrt{n}}\right)t_{1-\alpha/2;n-1}$. Substituting the sample statistic values and setting the quantity less than or equal to 1 yields $\left(\frac{2\sqrt{18.14}}{\sqrt{n}}\right)t_{0.975;n-1} \le 1$. Using trail and error for different values of *n,* it is easy to determine that $n = 280$ is the first value satisfying the equation: $\left(\frac{2\sqrt{18.14}}{\sqrt{280}}\right)1.9685 = 0.99954 \le 1$

However, the computations above are basically making the assumption that the variance of a larger sample would be consistent with that of the eight organizations in this study. Or in other words, that the population variance is known. Therefore using the computations below would be more appropriate, and can be seen to yield similar results.

$$\left(\frac{2\sigma}{\sqrt{n}}\right)z_{1-\alpha/2}\ ;\ \left(\frac{2\sqrt{18.14}}{\sqrt{n}}\right)z_{.975} \le 1\ ;\ \left(\frac{2\sqrt{18.14}}{\sqrt{n}}\right)1.96 \le 1\ ;\ 2\sqrt{18.14} = \frac{1}{1.96}\sqrt{n}\ ;$$

$\left(2\sqrt{18.14} * 1.96\right)^2 = n$, $n = 278$. Therefore a sample size of at least 278 should be sufficient to provide a 95% confidence interval, less than one unit wide, for the population mean. The model developed in this project can be used to assess the effectiveness of an organization's Internet management efforts. A more extension sample survey, given the appropriate time and resources, is necessary to provide the statistics required for more conclusive results when the model is applied in practice.

8 CONCLUSIONS AND RECOMMENDATIONS

Employees are traveling the Internet in record numbers these days, using the network to conduct business and communicate with coworkers, customers, and others. But as rapidly as the Internet is growing, it is also introducing new management, security and legal issues that many organizations have yet to address in their Internet policies.[21] This research developed, and demonstrated the use of, a model for assessing organizational Internet management policies. Some of the sampled organizations are further ahead than others with their Internet policies, but all realize the potential for problems and appear to be taking steps to improve. If organizations establish a policy using the Internet Use/Management Policy model described in this paper, they can begin to better manage their Internet access. In addition to policy, organizations can deploy software and hardware tools to further assist with this management challenge.

How did they compare?

Of the eight organizations reviewed in this project, the organizations with the best Internet policy are ODISC4, USACGSC, and MCUCSC. According to the Internet Use/Management policy model, these organizations' policies came closest to meeting all the criteria of the policy guideline. An assumption can be made that these organizations benefited from having the inherent knowledge of personnel with computer backgrounds.

The Pillsbury Corporation scored lowest of the eight organizations reviewed. They received no's particularly in the areas of higher precedence that caused their low score in the analysis. Pillsbury can correct these deficiencies by adding specific guidance to their policy. Also, as an additional measure, they could use software to provide "pop-up" messages that will reinforce the policy. Even though the areas where they performed poorly are important, they can be corrected with a rigorous policy awareness campaign.

---

[21] Weiss, Barry D, 1996, *Four Black Holes in Cyberspace*, Association Management, Volume 85, Issue 1 of Association Management Review, *30 January* 1996

What about PERSCOM?

PERSCOM scored above the mean. The comprehensive Internet policy that PERSCOM has strongly contributed to their high scores. The only areas where they need to improve are ownership of data and upload to the website. As a final measure, PERSCOM could require all users to sign a copy of the updated policy.

Recommendations:

As I mentioned earlier in this paper, due to limited scope and time constraints for completing this study, a small sample of organizations was surveyed. Regardless, comparing the sampled organizations is informative. PERSCOM scored below the mean in the analysis. The advice for their Internet policy is small. The only changes PERSCOM probably would need to make are subject of data ownership, procedures to upload to the website, and Internet use agreement. Neither deficiency should be considered critical, however, if the organization wants to have a completely effective Internet policy, they will need to put some guidelines for these subjects into their policies.

On the other hand, the Pillsbury Corporation, who scored lowest of the eight organizations, needs some significant improvements in their policies. The areas they need to improve are scope of policy, use of system, acceptance of policy, presumption of privacy and upload to website. Fortunately for Pillsbury these are probably the easiest to correct and manage. These criteria are all closely related and can be easily corrected by providing each user with two copies of the policy; one to keep and the other to sign, date and return to the system administrator to acknowledge having read and agreed to policy terms.[22] For Pillsbury, this would rectify two and possibly three of their identified deficiencies. However the Pillsbury Company is aware of their shortcomings, and has taken corrective measures to implement an effective Internet Use/Management policy.

The importance of an Internet policy for organizations in today's high technology world becomes more apparent every day. As more stories of inappropriate behavior such as the

---

[22] Wasch, Ken, 1997, *E-mail and Internet Policy*, Association Management, 1 May 1997, URL:

downloading of child pornography surface, more organizations will realize the importance of having a clearly stated Internet policy. The limited scope of this study provides a model and a framework for evaluating organizational Internet management policies but additional work is required to provide statistics that can be used on a large scale to make definitive conclusions for any particular organization.

<http://www.asaenet.org/newsletters/display/0,1901,249,00.html>, 15 October 2000

9 WORKS CITED

Administering Decency. Volume 19, Issue 34 of Infoworld, 25 August 1997.

Abbate, Janet, and Brian Kahin. *Standards Policy for Information Infrastructure*, Massachusetts: MIT Press, c1995, 635.

Attidore, Marilyn. Field Grade Career Manager PERSCOM. Interview by author, 21 December 2000.

Brown, Gary E. MAJ. Marine Corps Command and General Staff College, Interview by author, 5 January 2001.

Choo, Chun Wei, Information Management for the Intelligent Organization: *The Art of Scanning the Environment*, New Jersey, 1995, 255.

Customer Service Supervisor. Pillsbury Company, Email Interview by author 27 December 2000.

Davenport, Judy. Action Officer, Office of the Deputy Chief of Staff for Personnel (DCSPER), Interview by author, 5 January 2001.

Defense Information Systems Agency, *Director's Policy Letter 99-6, Information Services*, 5 September 1999

Elron Internet Manager, URL: http://www.elronsoftware.com/productfamily/overview.shtml>. Accessed 25 September 2000.

Farnell, Angie, MAJ. U.S. Army Command and General Staff College, Interview by author, 5 October 2000.

Fidelman, Miles R., *All-out Internet Access*, Illinois, American Library Association, 1997, 105.

Finney, Joseph B. CEO. Pauline & Duke Paralegal, Inc. Email Interview by author, 28 November 2000.

Get Management on Board First, Volume 18, Issue 34 of InfoWorld, 19 August 1996.

Greenland, Ron. Career Manager analyst PERSCOM. E-mail Interview by author, 14 December 2000.

Howard, John D. (1997). *An Analysis of Security Incidents on The Internet* 1989 - 1995. Ph.D. diss., Carnegie Mellon University.

Information Management , (AR 25-1), 15 February 15, 2000.

Information Systems Security, (AR 380-19), 27 February 1998.

Information Systems Security Monitoring, (AR 380-53), 29 April 1998.

Kahn, Brian and James Keller. *Public Access to the Internet*, Massachusetts: MIT Press, C1995, viii, 390.

King, James B. System Administrator Office of the Director of Information Systems for Command, Control, Communications (DISC4), Email Interview by author 26 December 00.

Mendenhall, William, and R. Lyman Ott. *Understanding Statistic,* Duxbury Press, c1994, 6th ed., 235.

Rensel, Harry. Information Management Officer, Office of the Director of Information Systems for Command, Control, Communications (DISC4), Email Interview by author 4 January 01.

Russell, Michel M. MAJ. Marine Corps Command and General Staff College, Interview by author, 28 December 2000.

Schwartau, Winn. Information Warfare: Chaos on the Information Superhighway. New York, New York: Thunder's Mouth Press, 1996.

Siyan, Karanjit. *Internet Firewalls and Network Security*, Indiana: New Riders Pub, c1995, 410.

A source, Defense Information Systems Agency, who wishes to remain anonymous. Email Interview by author 6 January 2001.

The Network Discusses: *Internet Policies, Rewards and Recognition, Compensation and Benefits Review*, March 1997, Volume 29, Issue 2

U.S. Total Army Personnel Command, PERSCOM Systems Security User Awareness Handbook, August 1999

Wasch, Ken. E-*mail and Internet Policy*, Association Management, 1 May 1997, URL: <http://www.asaenet.org/newsletters/display/0,1901,249,00.html>. Accessed 15 October 2000.

Weiss, Barry D. Four *Black Holes in Cyberspace*, Volume 85, Issue 1 of Association Management Review, *30 January* 1996

Wiggins, Richard. *The Internet for Everyone: A Guide for Users and Providers*, New York, c1995.

Williams, Mary. Budget Analyst Office of the Director of Information Systems for Command, Control, Communications (DISC4), Email Interview by author 15 December 00.

Wynder, Christopher. Military Police Future Readiness Officer PERSCOM. Interview by author, 21 December 2000.